



Teknik analisis keandalan sistem – Prosedur moda kegagalan dan analisis efek



Daftar isi

Daftar isi	i
Prakata	ii
1 Ruang lingkup	1
2 Umum.....	1
2.1 Tujuan analisis	2
2.2 Penerapan.....	2
3 Prinsip dasar MKAE	5
3.1 Terminologi.....	5
3.2 Konsep	5
3.3 Definisi struktur fungsional sistem	5
3.4 Informasi yang diperlukan untuk melaksanakan MKAE	6
3.5 Penggambaran struktur sistem	7
3.6 Moda kegagalan	7
3.7 Konsep kekritisian	9
3.8 Hubungan antara MKAE dan metoda analisis lainnya	9
4 Prosedur.....	10
4.1 Definisi sistem dan persyaratan	10
4.2 Pengembangan diagram blok	11
4.3 Penetapan aturan pokok	11
4.4 Moda, sebab dan efek kegagalan	12
4.5 Metoda deteksi kegagalan	14
4.6 Pernyataan kualitatif tentang kepentingan kegagalan dan ketentuan alternatif	14
4.7 Keterangan pada lembar kerja	14
5 Analisis kekritisian	14
5.1 Probabilitas moda kegagalan	15
5.2 Evaluasi kekritisian.....	15
6 Laporan analisis	15
Lampiran A Contoh moda kegagalan, efek dan analisis kekritisian	17
Lampiran B Contoh skala kekritisian efek kegagalan.....	18

Prakata

Standar Nasional Indonesia (SNI) mengenai “Teknik analisis keandalan sistem – Prosedur moda kegagalan dan analisis efek”, diadopsi dari standar *International Electrotechnical Commission* (IEC) 60812 (1985), dengan judul “*Analysis techniques for system reliability – Prosedur for failure mode and effects analysis (FMEA)*”.

Standar ini dirumuskan oleh Panitia Teknis Keandalan Sistem dan Peralatan Ketenagalistrikan (PTKS) masa kerja Tahun 2003.

Ketika dalam taraf Rancangan Standar Nasional Indonesia (RSNI), standar ini telah melalui proses/prosedur perumusan standar dan terakhir dibahas dalam Forum Konsensus XXII pada tanggal 11 sampai dengan 13 November 2003 untuk mencapai mufakat.



Teknik analisis keandalan sistem – Prosedur moda kegagalan dan analisis efek

1 Ruang lingkup

Standar ini menguraikan:

- Moda Kegagalan dan Analisis Efek (MKAE) dan
- Moda Kegagalan Analisis Efek dan Kekritisan (MKAEK).

Memberikan:

- petunjuk bagaimana dapat menerapkannya untuk mencapai berbagai tujuan.

Petunjuk tersebut sebagai berikut:

- dengan memberikan langkah-langkah secara prosedur yang diperlukan untuk melakukan analisis;
- dengan mengidentifikasi istilah yang tepat, asumsi, ukuran kekritisan, moda kegagalan;
- dengan menentukan prinsip dasar;
- dengan memberikan contoh formulir yang diperlukan.

Semua pertimbangan kualitatif umum yang disajikan untuk MKAE akan berlaku untuk MKAEK, karena yang satu merupakan kelanjutan dari yang lainnya.

2 Umum

MKAE dan MKAEK merupakan metoda analisis keandalan yang dimaksudkan untuk mengidentifikasi kegagalan yang mempunyai konsekuensi yang berarti yang mempengaruhi kinerja sistem pada penerapannya.

Umumnya, kegagalan atau moda kegagalan dari sembarang komponen akan mempunyai pengaruh buruk pada kinerja sistem. Dalam studi keandalan sistem, diperlukan analisis keselamatan dan ketersediaan, analisis kualitatif dan kuantitatif yang keduanya saling menunjang. Metoda analisis kuantitatif membolehkan kalkulasi atau perkiraan indeks kinerja sistem saat memenuhi satu tugas khusus atau pada operasi jangka panjang dalam kondisi khusus. Indeks tipikal menunjukkan keandalan, keselamatan, ketersediaan, laju kegagalan, waktu rata-rata efektif ke kegagalan/MTTF, dan lain-lain.

MKAE didasarkan pada ketersediaan tingkat komponen atau subrakitan tertentu tempat kriteria kegagalan dasar (moda kegagalan primer). Dengan memulai dari karakteristik kegagalan elemen dasar dan struktur sistem fungsionalnya, MKAE menentukan hubungan antara kegagalan elemen dan kegagalan sistemnya, malfungsi, keterbatasan operasi dan penurunan kinerja atau keterpaduan. Untuk mengevaluasi kegagalan sekunder, sistem, subsistem dan seterusnya, waktu urutan kejadian harus juga dipertimbangkan.

Dalam pandangan yang sempit, MKAE dibatasi pada analisis kualitatif moda kegagalan perangkat keras, tidak memasukkan kesalahan manusia dan kesalahan perangkat lunak, walaupun kenyataannya bahwa sistem yang sekarang ini biasanya terkena kedua-duanya. Dalam pandangan yang lebih luas, faktor tersebut dimasukkan.

Tingkat keparahan konsekuensi kegagalan digambarkan dengan kekritisan. Kekritisan ditandakan dengan kategori atau tingkatan yang merupakan fungsi dari bahaya dan

hilangnya/berkurangnya kemampuan sistem dan kadang-kadang fungsi dari probabilitas kejadian. Probabilitas ini paling baik diidentifikasi secara terpisah.

Kelanjutan yang logis dari MKAE adalah pertimbangan kekritisannya dan probabilitas kejadian dari moda kegagalan. Analisis kekritisannya dari moda kegagalan yang teridentifikasi ini secara luas dikenal dengan MKAEK.

2.1 Tujuan analisis

MKAE dan MKAEK merupakan teknik yang penting untuk satu program jaminan keandalan yang dapat diterapkan pada masalah yang luas dan dapat ditemui pada sistem teknik dengan berbagai pendalaman dan modifikasi untuk memenuhi tujuannya. Analisis dilaksanakan secara terbatas selama fase pembuatan konsep, fase perancangan dan fase pendefinisian dan lebih dalam lagi selama fase desain dan pengembangan. Namun penting untuk diingat bahwa MKAE hanya bagian dari program keandalan dan mampu-rawat yang memerlukan banyak tugas dan aktifitas yang berbeda. MKAE merupakan metode penyimpulan pelaksanaan keandalan sistem kualitatif atau analisis keselamatan dari tingkat rendah sampai tingkat yang tinggi.

Pengembangan diagram blok keandalan dan diagram keadaan yang diambil dari struktur sistem disalinghubungkan dengan menggunakan MKAE. Masing-masing diagram akan dibutuhkan untuk:

- kriteria yang diidentifikasi dan ditentukan secara berbeda untuk kegagalan sistem;
- penurunan fungsi atau pengurangan jaminan fungsi;
- keselamatan;
- fase operasi alternatif.

Tujuan MKAE dan MKAEK dapat mencakup:

- a) evaluasi pengaruh dan urutan kejadian yang disebabkan oleh masing-masing moda kegagalan barang yang teridentifikasi dari sebab apapun pada berbagai tingkat dari hirarki fungsi sistem;
- b) penentuan seberapa pentingnya atau kekritisannya dari masing-masing moda kegagalan terhadap fungsi atau kinerja yang benar dari sistem dan dampak pada keandalan dan/atau keselamatan proses terkait;
- c) klasifikasi moda kegagalan teridentifikasi menurut mampu-deteksi, mampu-diagnosa, mampu-uji, mampu-ganti barang, kelengkapan kompensasi dan operasi (perbaikan, pemeliharaan dan perbekalan, dan lain-lain) dan karakteristik lainnya yang terkait.
- d) estimasi ukuran tingkat kepentingan dan probabilitas kegagalan, tergantung pada ketersediaan data.

2.2 Penerapan

2.2.1 Bidang penerapan MKAE

MKAE adalah suatu metoda yang diadaptasi terutama untuk studi kegagalan bahan dan perlengkapan dan yang dapat diterapkan pada kategori sistem berdasarkan atas teknologi yang berbeda (listrik, mekanik, hidrolik, dan lain-lain) dan gabungan teknologi. MKAE dapat juga digunakan untuk studi perangkat lunak dan kinerja manusia.

2.2.2 Penerapan MKAE dalam kerangka kerja proyek

Pengguna sebaiknya menentukan bagaimana dan untuk tujuan apa dia menggunakan MKAE dalam disiplin tekniknya dia sendiri. Dapat digunakan sendiri atau untuk melengkapi dan menunjang metoda analisis keandalan lainnya. Persyaratan untuk MKAE bersumber dari kebutuhan untuk memahami perilaku perangkat keras dan implikasinya untuk operasi sistem atau perlengkapan. Kebutuhan untuk MKAE dapat bervariasi secara luas dari satu proyek ke proyek yang lain.

MKAE merupakan satu teknik untuk penunjang tinjau-ulang desain dan untuk jaminan dan penilaian yang sebaiknya digunakan sejak langkah pertama desain sistem dan subsistem. MKAE tepat untuk semua tingkat desain sistem. Diperlukan training khusus untuk personil yang melaksanakan MKAE dan mereka harus mempunyai kerjasama yang erat dengan pendesain dan *engineer* sistem. MKAE harus diperbaharui karena proyek terus berjalan dan karena desain dimodifikasi. Pada akhir proyek, MKAE digunakan untuk memeriksa desain proyek tersebut dan dapat digunakan untuk menunjukkan kesesuaian sistem yang didesain dengan standar yang dipersyaratkan, peraturan dan persyaratan pengguna.

Informasi dari MKAE mengidentifikasi urutan prioritas untuk kendali proses dan uji inspeksi selama pembuatan dan pemasangan, dan untuk kualifikasi, persetujuan, uji penerimaan dan uji pemanasan. Hal ini memberikan informasi yang mendasar untuk prosedur diagnosa dan prosedur pemeliharaan.

Dalam memutuskan cakupan dan cara bagaimana MKAE sebaiknya diterapkan pada suatu barang atau desain, seseorang sebaiknya mempertimbangkan tujuan khusus yang dibutuhkan dari hasil MKAE, penjadualan waktu dengan aktifitas yang lain, dan seberapa penting dalam menetapkan tingkat kewaspadaan dan kendali yang ditentukan sebelumnya dari moda dan efek kegagalan yang tidak diinginkan. Hal ini dapat mengarah ke perancangan MKAE secara kualitatif pada tingkat tertentu (sistem, subsistem, komponen, subkomponen) untuk menghubungkan dengan desain yang berulang dan proses pengembangan.

Untuk memastikan bahwa ini efektif, maka MKAE harus dikenal dalam program keandalan.

2.2.3 Penggunaan MKAE

Beberapa penerapan rinci dan keuntungan dari MKAE adalah sebagai berikut:

- a) untuk mengidentifikasi kegagalan yang apabila terjadi sendirian, mempunyai efek yang tidak dapat diterima atau yang berarti dan untuk menentukan moda kegagalan yang dapat mempengaruhi secara serius operasi yang diharapkan atau operasi yang diperlukan. Efek tersebut dapat berupa kegagalan berikutnya;
- b) menentukan kebutuhan untuk:
 - menghindari duplikasi;
 - mendesain keistimewaan yang dapat menambah probabilitas “gagal tetapi tetap aman” hasil kegagalan;
 - penurunan tingkat lebih lanjut dan/atau penyederhanaan desain;
- c) untuk menentukan kebutuhan terhadap bahan, bagian, gawai dan komponen alternatif;
- d) mengidentifikasi konsekuensi kegagalan yang serius dan selanjutnya kebutuhan untuk tinjau ulang dan revisi desain;

- e) menyediakan model logik yang diperlukan untuk mengevaluasi probabilitas anomali kondisi operasi dari sistem;
- f) untuk memberitahukan bahaya keselamatan dan daerah kemungkinan bermasalah, atau ketidaksesuaian dengan persyaratan peraturan;
- g) untuk memastikan bahwa program uji dapat mendeteksi moda kegagalan yang potensial;
- h) untuk membuat siklus tugas yang dapat mengantisipasi dan menghindari kegagalan karena aus;
- i) untuk memfokuskan pada daerah kunci, tempat untuk mengkonsentrasikan kualitas, inspeksi dan kendali proses pembuatan;
- j) untuk menghindari modifikasi yang mahal dengan identifikasi dini pada desain yang kurang sempurna;
- k) untuk menetapkan kebutuhan untuk pencatatan dan pemantauan data selama pengujian, pemeriksaan dan penggunaan;
- l) untuk memberikan informasi untuk pemilihan titik pemeliharaan preventif atau korektif dan pengembangan petunjuk pemecahan masalah, perlengkapan uji pasangan dalam dan titik uji yang sesuai;
- m) untuk memfasilitasi atau menunjang penentuan kriteria uji, rancangan uji dan prosedur diagnosa, misalnya pengujian kinerja, pengujian keandalan;
- n) untuk mengidentifikasi sirkit yang memerlukan analisis kasus terburuk (sering diperlukan untuk moda kegagalan yang menyangkut parameter yang tidak terkendali);
- o) untuk menunjang desain urutan pemisahan gangguan dan untuk menunjang perancangan untuk moda operasi alternatif dan konfigurasi ulang;
- p) untuk memfasilitasi komunikasi antar:
 - enjinir umum dan enjinir spesialis (*General and specialized engineers*);
 - pabrikan perlengkapan dan pemasok;
 - pengguna sistem dan pendesain atau pabrikan;
- q) untuk meningkatkan pengetahuan dan pemahaman analis terhadap perilaku perlengkapan yang telah dipelajari;
- r) untuk memberikan pendekatan yang sistematis dan benar pada studi fasilitas sistem.

2.2.4 Keterbatasan dan kekurangan MKAE

MKAE sangat efisien jika diterapkan pada analisis elemen yang menyebabkan kegagalan sistem keseluruhan.

Namun, MKAE dapat sangat sulit dan melelahkan serta membosankan untuk kasus sistem yang kompleks yang mempunyai fungsi banyak dan terdiri dari sejumlah komponen. Hal ini disebabkan banyaknya informasi sistem yang terinci yang harus dipertimbangkan. Kesukaran ini dapat bertambah dengan jumlah kemungkinan moda operasi, juga dengan pertimbangan kebijakan perbaikan dan pemeliharaan.

Keterbatasan lain adalah akibat kesalahan manusia yang biasanya tidak dimasukkan. Studi tentang interaksi manusia mesin merupakan subyek dari metoda khusus (misalnya analisis tugas). Umumnya, kesalahan manusia muncul selama operasi sistem dalam moda yang berurutan dan studi tentang dampaknya harus dibuat dengan metoda seperti misalnya analisis sebab-akibat. Meskipun demikian, MKAE dapat mengidentifikasi komponen yang paling peka terhadap kesalahan manusia. Keterbatasan selanjutnya kelihatan jika pengaruh lingkungan berarti. Pertimbangan tentang pengaruh tersebut memerlukan pengetahuan yang menyeluruh tentang karakteristik dan kinerja komponen yang berbeda dari sistem.

Harus dicatat bahwa kesalahan manusia dan pengaruh lingkungan merupakan sebab sebagian besar sumber kegagalan moda yang umum atau sebab yang umum. Pernyataan ini akan dibahas dalam subayat 3.6.1.

3 Prinsip dasar MKAE

3.1 Terminologi

Semua terminologi kecuali yang diidentifikasi secara khusus sudah sesuai dengan Publikasi IEC 271: Daftar Istilah Dasar, Definisi dan Matematik yang terkait untuk Keandalan.

3.2 Konsep

MKAE memerlukan:

- sistem dirinci kedalam “elemen”;
- diagram struktur fungsional sistem dan identifikasi berbagai data yang diperlukan untuk melaksanakan MKAE;
- konsep moda kegagalan;
- konsep kekritisian (jika analisis kekritisian diperlukan);

Pada akhirnya dan sebelum prosedur penerapan MKAE diuraikan lebih jelas, harus ditentukan hubungan yang sekarang ada antara MKAE (dan MKAEK) dan metoda analitis kualitatif (dan kuantitatif) lainnya.

3.3 Definisi struktur fungsional sistem

Analisis diawali dengan memilih tingkat paling rendah diinginkan yang (biasanya tingkat bagian, sirkuit, atau modul) dimana tersedia informasi yang memadai. Pada tingkat ini, berbagai moda kegagalan yang dapat terjadi untuk masing-masing barang pada tingkat tersebut ditabulasikan. Efek kegagalan terkait dari masing-masing, diambil satu demi satu dan secara bergantian, diinterpretasikan sebagai satu moda kegagalan untuk pertimbangan efek kegagalan pada tingkat fungsional selanjutnya yang lebih tinggi. Pengulangan yang berurutan menghasilkan pengidentifikasian efek kegagalan yang terkait dengan moda kegagalan spesifik pada semua tingkat fungsional yang diperlukan sampai ke sistem atau tingkat yang paling tinggi.

Perlu menentukan tingkat rincian yang akan digunakan untuk analisis. Misalnya, sistem dapat dirinci dalam subsistem, barang paling sedikit diganti, atau bagian detail (komponen). Jika terkait, barang non-listrik harus dipertimbangkan. Jika diperlukan hasil kuantitatif, tingkat yang dipilih harus yang memungkinkan untuk mendapatkan data laju kegagalan pada setiap moda kegagalan atau moda kesalahan yang cukup (dan dapat diharapkan) atau untuk membuat asumsi yang diketahui beralasan dari laju kegagalan tersebut. Tingkat rincian yang dipilih memerlukan pengetahuan yang dapat diandalkan dan mendetail tentang moda kegagalan dari elemen. Selain dari persyaratan ini, tidak mungkin ataupun tidak dikehendaki untuk menetapkan aturan yang tegas tentang pemilihan tingkat rincian.

3.4 Informasi yang diperlukan untuk melaksanakan MKAE

3.4.1 Struktur sistem

Diperlukan informasi berikut:

- elemen sistem yang berbeda beserta karakteristik, kinerja, peran dan fungsi mereka;
- hubungan antar elemen;
- tingkat redundansi dan sifat dari sistem yang redundan;
- letak sistem terhadap keseluruhan.

Diperlukan data yang terkait dengan fungsi, karakteristik dan kinerja untuk semua tingkat yang dipertimbangkan sampai dengan tingkat yang paling tinggi.

3.4.2 Inisiasi, operasi, kendali dan pemeliharaan sistem

Status kondisi operasi yang berbeda dari sistem harus ditetapkan, juga perubahan dalam konfigurasi atau posisi sistem dan komponennya selama fase operasinal yang berbeda. Kinerja minimum yang diminta dari sistem harus ditentukan dan persyaratan khusus tersebut seperti ketersediaan atau keselamatan harus dipertimbangkan sebagai tingkat kinerja yang ditentukan dan tingkat kerusakan atau celaka.

Wajib untuk diketahui:

- durasi dari masing-masing tugas;
- selang waktu antara uji berkala;
- waktu yang tersedia untuk koreksi sebelum konsekuensi yang serius terjadi pada sistem;
- fasilitas keseluruhan, lingkungannya dan/atau personilnya;
- kondisi perbaikan termasuk koreksi dan waktu, perlengkapan dan/atau personil untuk menyelesaikannya.

Diperlukan informasi selanjutnya pada:

- prosedur operasi selama *start-up* sistem;
- kendali selama fase operasional;
- pemeliharaan secara preventif dan/atau pembetulan;
- jika dilakukan, prosedur untuk uji rutin.

3.4.3 Lingkungan sistem

Kondisi lingkungan sistem harus ditetapkan, termasuk kondisi ambien dan yang dibuat oleh sistem lain didalam fasilitas. Sistem harus digambarkan sebagaimana hubungannya, ketergantungannya, atau interkoneksi dengan sistem bantu atau sistem lain dan dengan manusia.

Pada tahap desain biasanya kenyataan tersebut tidak diketahui sehingga akan diperlukan perkiraan dan asumsi. Selama proyek berjalan terus, data akan harus diperbanyak dan MKAE dimodifikasi untuk memungkinkan adanya informasi baru atau asumsi atau perkiraan yang dirubah.

MKAE atau analisis lainnya memerlukan pemodelan tertentu dari sistem, yaitu penyederhanaan informasi yang terkait pada sistem. Dapat dibuat beberapa asumsi tentang sifat moda kegagalan dan keseriusan akibatnya. Misalnya, pada studi keselamatan dapat dibuat hipotesa konservatif yang menyangkut dampak kegagalan tertentu pada sistem.

MKAE yang dilaksanakan pada perangkat keras dapat menghasilkan keputusan pada probabilitas efek, probabilitas kekritisitas dan probabilitas bersyarat yang melibatkan pengidentifikasian elemen perangkat lunak dan urutan dan penjadwalan waktunya. Jika hal ini yang terjadi, maka fakta harus diidentifikasi secara jelas karena setiap perubahan berikutnya atau perbaikan perangkat lunak dapat memodifikasi MKAE dan penilaiannya. Persetujuan pengembangan dan perubahan perangkat lunak dapat tergantung pada revisi MKAE dan penilaian yang terkait.

3.5 Penggambaran struktur sistem

Penggambaran struktur dan operasi sistem dengan simbol, khususnya diagram dapat digunakan. Biasanya diagram blok dipilih untuk menampilkan lebih jelas semua fungsi yang penting bagi sistem.

Dalam diagram, blok dihubungkan bersama dengan menggunakan garis yang menggambarkan masukan dan keluaran setiap fungsi. Biasanya sifat dari masing-masing fungsi dan masing-masing masukan harus diuraikan secara tepat. Beberapa diagram dapat mencakup tahapan yang berbeda dari operasi sistem.

Umumnya, penyajian grafis termasuk yang terkait erat dengan metoda analisis, seperti pohon kegagalan, atau diagram sebab-akibat, menyumbangkan pemahaman yang lebih baik tentang sistem, strukturnya dan operasinya. Namun kegunaannya menimbulkan masalah pada hubungan antara MKAE dan metoda ini; hal ini akan dibahas dalam subayat 3.8.

3.6 Moda kegagalan

Moda kegagalan adalah efek dari kegagalan yang diobservasi pada komponen sistem.

Semua moda kegagalan yang mungkin atau berpotensi dari sistem perlu didaftar sebagai dasar yang penting untuk MKAE. Pembuat komponen atau perlengkapan sebaiknya berperan serta dalam pengidentifikasian moda kegagalan produknya dengan kejelasan sebagai berikut:

- untuk komponen baru, dapat mengacu pada komponen lain dengan fungsi dan struktur yang mirip dan pada pengujian yang dilaksanakan pada komponen lain tersebut;
- untuk komponen yang sudah digunakan secara umum dalam pelayanan, catatan kinerja, kegagalan yang dilaporkan dan uji laboratorium dapat digunakan untuk pembandingan;
- komponen rumah yang dapat dirinci kedalam elemen dapat dianalisis secara kualitatif dengan memperlakukan masing-masing sebagai satu sistem;
- moda kegagalan yang berpotensi dapat diuraikan dari fungsi dan tipikal parameter fisik yang tipikal dari operasi komponen.

Sebaiknya moda kegagalan diklasifikasikan. Dua cara umum untuk mengklasifikasikan moda kegagalan adalah:

- a) pengidentifikasian moda kegagalan umum, seperti yang diambil dari definisi keandalan (lihat Tabel I);
- b) dengan membuat daftar selengkap mungkin semua moda kegagalan yang generik (lihat Tabel II).

3.6.1 Kegagalan Moda Umum (sebab umum) (KMU)

Dalam analisis keandalan, tidak cukup mempertimbangkan hanya kegagalan acak dan kegagalan sendiri-sendiri. Beberapa KMU dapat terjadi, yang menyebabkan penurunan atau kegagalan kinerja sistem melalui kekurangan yang serentak pada beberapa komponen sistem, disebabkan oleh sumber tunggal seperti kesalahan desain, kesalahan manusia, dan lain-lain.

KMU merupakan hasil dari kejadian yang karena ada ketergantungan, menyebabkan bersamaannya beberapa keadaan kegagalan pada dua atau lebih kegagalan komponen (tidak termasuk kegagalan sekunder yang disebabkan oleh efek kegagalan primer).

KMU dapat dikenai teknik analitis kualitatif dengan menggunakan MKAE. karena MKAE merupakan prosedur untuk memeriksa masing-masing moda kegagalan dan penyebab yang terkait secara berurutan dan juga untuk mengidentifikasi semua uji berkala, tindakan pemeliharaan preventif dll, maka memungkinkan satu studi tentang semua penyebab yang dapat menyebabkan adanya KMU berpotensi.

Penyebab tersebut dapat diklasifikasikan kedalam lima kategori utama:

- a) pengaruh lingkungan (normal, abnormal, dan tidak sengaja);
- b) desain kurang baik;
- c) cacat pabrik;
- d) kesalahan rakitan;
- e) kesalahan manusia (selama operasi dan/atau pemeliharaan).

Daftar pemeriksaan berdasarkan kategori tersebut diatas dapat digunakan untuk mengidentifikasi secara rinci semua kemungkinan penyebab yang dapat mengakibatkan adanya KMU.

Redundansi sendiri tidak memecahkan masalah KMU. Gabungan dari beberapa metoda dapat berguna dalam membahas kegagalan berikut: diversitas fungsi, redundansi dari jenis yang berbeda, pemisahan secara fisik, pengujian dan lain-lain. Daftar pemeriksaan seperti diatas dapat digunakan untuk memeriksa keterkaitan dan keefektifan masing-masing metoda. Pemeriksaan tindakan preventif terhadap KMU diluar lingkup MKAE.

3.6.2 Faktor manusia

Beberapa sistem harus didesain untuk membolehkan beberapa kesalahan manusia, misalnya dengan melengkapi silih kunci mekanis pada sinyal kereta api, kata kunci (*password*) untuk penggunaan komputer atau pengambilan data. Jika kelengkapan tersebut ada didalam sistem, maka efek kegagalan kelengkapan tersebut akan tergantung pada jenis kesalahan. Beberapa moda kesalahan manusia sebaiknya dipertimbangkan untuk selain sistem bebas gangguan, untuk memeriksa keefektifan kelengkapan tersebut. Walaupun belum lengkap, tetapi membuat daftar dari sebagian moda ini sudah berguna.

3.6.3 Kesalahan perangkat lunak

Malfungsi karena kesalahan atau kekurangcukupan dari perangkat lunak akan mempunyai efek yang kekritisannya akan ditentukan oleh desain perangkat keras dan perangkat lunak. Pengakuan adanya kesalahan atau kekurangcukupan tersebut dan analisis efeknya memungkinkan, hanya dalam cakupan yang terbatas dan ini diluar lingkup MKAE. Namun, efek pada perangkat keras dari kesalahan yang mungkin dalam perangkat lunak dapat diperkirakan.

3.7 Konsep kekritisian

Tingkat kekuatiran yang tepat terhadap setiap situasi gangguan terkait secara jelas dengan probabilitas kejadian dan keseriusan efeknya. Konsep kekritisian menunjukkan banyaknya analisis dan melengkapi MKAE. Tidak ada kriteria umum untuk kekritisian yang dapat diterapkan pada suatu sistem, karena konsep ini terangkai secara fundamental dengan kekritisian tingkatan konsekuensi dan probabilitas kejadiannya. Tingkatan konsep sendiri dapat didefinisikan dalam beberapa macam tergantung apakah tujuannya terkait dengan keselamatan, konsekuensi kerusakan atau kehilangan, atau ketersediaan pelayanan.

Konsep kekritisian banyak menambah kegunaan proses MKAE dengan mempertimbangkan:

- hal dipelajari lebih intensif untuk menghilangkan bahaya khusus, untuk menambah probabilitas hasil “gagal selamat” atau mengurangi laju atau cakupan kegagalan dan risiko akibat kerusakan;
- hal yang memerlukan perhatian khusus selama pembuatan dan kendali mutu yang ketat, atau kendali khusus pada waktu penanganan;
- persyaratan khusus dalam spesifikasi pembelian yang menyangkut desain, kinerja, keandalan, keselamatan, atau jaminan mutu;
- standar penerimaan untuk produk dari subkontraktor termasuk parameter yang sebaiknya diuji secara ketat;
- setiap prosedur khusus, pelindung, perlengkapan proteksi, gawai pemantau, atau sistem peringatan;
- penerapan biaya yang paling efektif pada sumber daya pencegahan kecelakaan.

Supaya dapat mendefinisikan kekritisian, maka diperlukan skala untuk menilai tingkat redundansinya dengan mengacu pada kriteria yang dipertimbangan. Lampiran B memberikan contoh klasifikasi tingkat konsekuensi dalam empat tingkatan utama. Tingkat sebenarnya yang dipilih sangat bebas. Dalam contoh sekarang, tingkat tersebut didasarkan atas gabungan kriteria yang dianggap terkait, dan masing-masing yang menyangkut:

- mencelakakan personil (luka-luka, kematian);
- kehilangan fungsi sistem;
- dampak lingkungan dan kerusakan bahan.

Istilah “katastrofis”, “kritis”, “major”, “minor” sering digunakan tetapi definisinya dalam Publikasi IEC 271 dapat sesuai atau tidak sesuai dengan penggunaan MKAE tertentu. Kata seperti tersebut diatas dapat didefinisikan secara spesifik dalam masing-masing studi terkait.

3.8 Hubungan antara MKAE dan metoda analisis lainnya

Perlu didiskusikan bagaimana metoda analisis yang berbeda keandalan sistem dan ketersediaan sistem digabung dalam satu proyek.

MKAE (atau MKAEK) dapat digunakan sendiri. Sebagai metoda penyimpulan yang sistematis, MKAE paling sering digunakan untuk melengkapi pendekatan lainnya, khususnya metoda urai. Pada tahap desain, sering sukar untuk memutuskan apakah pendekatan penyimpulan atau pendekatan yang menonjol, karena keduanya digabung dalam proses pemikiran dan analisis. Jika tingkat risiko ditemukan dalam sistem dan fasilitas industri,

maka pendekatan penyimpulan yang lebih disukai dan selanjutnya MKAE merupakan perkakas desain yang penting. Namun sebaiknya dibantu dengan metoda lain terutama jika kegagalan multipel dan efek yang berurutan harus dipelajari.

Sesuai dengan program proyek, satu metoda dapat dikembangkan sebelum lainnya. Selama tahap desain dini, walaupun hanya fungsi, struktur sistem umum dan subsistem sudah didefinisikan, kinerja yang baik atau jalur kegagalan dari sistem dapat digambarkan masing-masing dalam diagram blok keandalan atau pohon kegagalan. Namun, untuk membantu menggambar diagram sistem ini, proses penyimpulan MKAE sebaiknya diterapkan pada subsistem sebelum didesain. Dalam keadaan ini, pendekatan MKAE tidak dapat berupa serangkaian prosedur tetapi sebagai gantinya satu proses pemikiran yang tidak mudah diidentifikasi dalam bentuk tabel. Umumnya, saat menganalisis sistem yang kompleks yang melibatkan beberapa fungsi, banyak komponen dan saling hubung antara komponen tersebut, ternyata MKAE penting tetapi tidak cukup.

4 Prosedur

Banyaknya variasi dalam kekomplekan desain dan penerapan sistem dapat memerlukan pengembangan masing-masing MKAE yang konsisten dengan informasi yang tersedia. Berikut langkah dasar yang digunakan dalam studi MKAE:

- a) pendefinisian sistem dan persyaratan operasi fungsional dan minimalnya;
- b) pengembangan fungsi dan diagram blok keandalan serta model dan uraian diagramatis atau matematis lainnya;
- c) penetapan prinsip dasar dan dokumentasi terkait dalam melaksanakan analisis;
- d) pengidentifikasian moda kegagalan, penyebab dan efeknya, seberapa pentingnya, dan urutannya;
- e) pengidentifikasian deteksi kegagalan, ketentuan dan metoda isolasi;
- f) pengidentifikasian ketentuan desain dan operasi, khususnya terhadap kejadian yang tidak diinginkan;
- g) penentuan kekritisitas kejadian (hanya MKAEK);
- h) evaluasi probabilitas kegagalan (hanya MKAEK);
- i) pencarian kombinasi spesifik dari kegagalan multipel yang harus dipertimbangkan (tidak wajib);
- j) rekomendasi.

Prosedur MKAE dapat dilaksanakan dengan atau tanpa analisis kekritisitas. Jika tanpa, analisis kekritisitas, maka langkah g) dan h) dihilangkan.

4.1 Definisi sistem dan persyaratannya

4.1.1 Pendefinisian sistem

Definisi lengkap dari sistem mencakup fungsi primer dan sekundernya, penggunaannya, kinerja yang diharapkan, keterbatasan sistem dan kondisi eksplisit yang ikut menyebabkan kegagalan. Karena setiap sistem yang diberikan didesain untuk satu atau lebih moda operasi dan dapat bekerja selama beragam periode dalam waktu operasi sistem, maka definisi sistem sebaiknya juga mencakup beberapa uraian fungsional tentang operasi sistem untuk masing-masing moda dan durasinya.

4.1.2 Pendefinisian persyaratan fungsional

Perlu untuk mendefinisikan kedua-duanya, kinerja fungsional yang dapat diterima secara keseluruhan dan kinerja fungsional sistem elemen pembentuknya juga karakteristik kinerja yang dianggap tidak dapat diterima. Persyaratan fungsional sebaiknya termasuk definisi kinerja yang dapat diterima untuk semua karakteristik yang diinginkan dan dispesifikasikan, pada semua moda operasi dan non operasi, untuk semua perioda waktu yang terkait, dan untuk semua kondisi lingkungan.

4.1.3 Pendefinisian persyaratan lingkungan

Lingkungan tempat sistem diharapkan berfungsi, dipaparkan atau disimpan, sebaiknya didefinisikan secara jelas dan kinerja yang diharapkan pada masing-masing lingkungannya sebaiknya dispesifikasikan. Lingkungan dapat termasuk faktor seperti suhu, kelembaban, radiasi, getaran dan tekanan. Untuk sistem yang berhubungan dengan kehidupan manusia dan mesin (*cybernetic*), sebaiknya dipertimbangkan faktor lainnya, psikologis, fisiologis dan lingkungan sejauh dapat mempengaruhi kinerja manusia dan desain atau operasi sistem.

4.1.4 Persyaratan peraturan

Dalam mendefinisikan persyaratan sistem, sebaiknya dipertimbangkan semua persyaratan peraturan yang dapat diterapkan dan yang mempengaruhi produksi, penggunaan, samping produk samping operasi dan faktor lain yang akan mempengaruhi desain sistem.

4.2 Pengembangan diagram blok

Diagram yang menunjukkan elemen fungsional dari sistem diperlukan untuk pemahaman teknis dari fungsinya dan analisis sesudahnya.

Diagram sebaiknya menunjukkan setiap hubungan seri dan hubungan yang redunden antar elemennya dan saling ketergantungan fungsional diantara mereka. Hal ini memungkinkan kegagalan fungsional ditelusuri didalam sistem. Lebih dari satu diagram dapat diperlukan untuk menunjukkan moda operasi sistem alternatif. Diagram logik yang terpisah dapat disyaratkan untuk setiap moda operasi. Minimal diagram blok sebaiknya berisi:

- rincian sistem ke dalam subsistem utama termasuk hubungan fungsional;
- semua masukan dan keluaran yang berlabel dengan tepat dan nomor identifikasi yang diacu secara konsisten oleh setiap subsistem;
- semua redundansi, jalur sinyal alternatif dan ciri teknik lain yang memberikan tindakan "gagal – tetapi tetap aman".

4.3 Penetapan aturan pokok

4.3.1 Tingkat analisis

Prinsip dasar pemilihan tingkat sistem untuk analisis tergantung pada hasil yang dikehendaki dan ketersediaan informasi desain. Dapat digunakan petunjuk berikut:

- tingkat sistem tertinggi dipilih dari konsep desain dan persyaratan keluaran yang ditentukan;
- tingkat sistem terendah tempat analisis efektif merupakan tingkat yang tersedia informasi untuk menetapkan definisi dan uraian fungsi. Tingkat sistem terendah dipengaruhi oleh pengalaman sebelumnya. Analisis yang kurang rinci dapat dibenarkan untuk setiap sistem yang mempunyai desain yang sempurna, keandalan yang baik,

mampu-rawat dan catatan keselamatan. Sebaliknya, tingkat sistem yang lebih rendah dan lebih rinci ditunjukkan oleh setiap sistem dengan desain baru dan sistem dengan riwayat keandalan yang tidak diketahui;

- c) tingkat perbaikan dan pemeliharaan yang ditentukan atau diinginkan dapat menjadi petunjuk yang berharga dalam menentukan tingkat sistem yang lebih rendah. Tingkat sistem terendah tempat pemeliharaan sistem akan dilaksanakan sebaiknya diidentifikasi terlebih dahulu (identifikasi "elemen yang paling sedikit diganti"). Analisis kemudian dibuat dari tingkat tepat di atas tingkat sistem terendah tempat pemeliharaan akan dilaksanakan. Pada elemen sistem yang kritis, analisis dibuat sampai dengan elemen yang paling sedikit diganti.

4.3.2 Dokumentasi MKAE

Akan sangat membantu jika MKAE dibuat diatas formulir kertas kerja yang didesain secara khusus untuk sistem yang sedang dipelajari dan yang konsisten dengan tujuannya. Formulir tersebut biasanya disusun menurut kolom seperti terlihat pada Lampiran A. Informasi yang dimasukkan kedalam kolom biasanya:

- a) nama dari elemen sistem yang sedang dianalisis;
- b) fungsi yang dilaksanakan oleh elemen sistem;
- c) nomer identifikasi dari elemen sistem;
- d) moda kegagalan;
- e) sebab kegagalan;
- f) efek kegagalan;
- g) metoda deteksi kegagalan;
- h) pernyataan kualitatif dari seberapa penting kegagalan dan ketentuan alternatif;
- i) keterangan;

Dalam hal MKAEK, formulir kertas kerja dapat ditambah dengan:

- j) kekritisian;
- k) probabilitas kegagalan.

4.4 Moda, sebab dan efek kegagalan

Operasi yang berhasil dari suatu sistem tergantung pada kinerja elemen sistem kritis tertentu. Kunci untuk evaluasi kinerja sistem adalah pengidentifikasian elemen yang kritis. Prosedur untuk mengidentifikasi moda, penyebab dan efek kegagalan dapat diintensifkan secara efektif dengan persiapan daftar moda kegagalan yang telah diantisipasi dengan memperhitungkan:

- penggunaan sistem;
- elemen sistem khusus yang terlibat;
- moda operasi;
- spesifikasi operasi yang terkait;
- keterbatasan waktu;
- lingkungan.

Dalam MKAE definisi moda kegagalan, sebab kegagalan, efek kegagalan tergantung pada tingkat analisis. Pada saat analisis berlangsung, efek kegagalan yang teridentifikasi pada tingkat lebih rendah dapat menjadi moda kegagalan pada tingkat yang lebih tinggi. Serupa dengan ini, moda kegagalan pada tingkat lebih rendah dapat menjadi sebab kegagalan pada tingkat yang lebih tinggi, dan seterusnya.

4.4.1 Moda kegagalan

Daftar moda kegagalan umum diberikan pada Tabel I.

Hampir setiap jenis moda kegagalan dapat diklasifikasikan dalam satu kategori atau lebih. Kategori moda kegagalan umum ini mempunyai lingkup terlalu luas untuk analisis yang pasti; konsekuensinya dirinci seperti terlihat pada Tabel II. Moda kegagalan yang terdaftar pada tabel II dapat menguraikan kegagalan setiap elemen sistem dalam cara spesifik yang memadai. Jika digunakan bersama dengan spesifikasi kinerja yang mempengaruhi masukan dan keluaran pada diagram blok keandalan, semua moda kegagalan yang potensial dapat diidentifikasi dan diuraikan.

4.4.2 Penyebab kegagalan

Penyebab yang mungkin yang terkait dengan masing-masing moda kegagalan yang dianggap penting diidentifikasi and diuraikan. Penyebab setiap moda kegagalan diidentifikasi untuk dapat memperkirakan probabilitas kejadiannya, untuk mengetahui efek sekunder dan untuk menemukan tindakan perbaikan yang direkomendasikan. Karena satu moda kegagalan dapat mempunyai lebih dari satu penyebab, maka semua penyebab independen dan berpotensi untuk masing-masing moda kegagalan harus diidentifikasi dan diuraikan. Penyebab kegagalan di dalam tingkat sistem didekatnya juga dipertimbangkan.

Daftar dalam Tabel II memberikan definisi lebih spesifik dari moda kegagalan dan sebab kegagalan. Jadi misalnya, satu suplai daya dapat mempunyai suatu moda kegagalan umum yang diuraikan sebagai "kegagalan selama operasi", moda kegagalan spesifiknya "kehilangan keluaran" (29), dan salah satu sebab kegagalan "terbuka (listrik)" (31).

4.4.3 Efek kegagalan

Akibat dari masing-masing moda kegagalan yang diasumsikan pada operasi, fungsi, atau status elemen sistem diidentifikasi, dievaluasi dan dicatat. Pemeliharaan, personil dan tujuan sistem sebaiknya juga dipertimbangkan jika terkait. Efek kegagalan berfokus pada elemen sistem spesifik didalam diagram blok yang sedang dianalisis yang dipengaruhi oleh kegagalan dalam pertimbangan.

Efek kegagalan dapat mempengaruhi tingkat lebih tinggi berikutnya dan akhirnya tingkat tertinggi dalam analisis. Karena itu efek kegagalan pada setiap tingkat yang lebih tinggi sebaiknya dievaluasi.

4.4.3.1 Efek lokal

Istilah "efek lokal" mengacu pada efek moda kegagalan pada elemen sistem yang sedang dipertimbangan. Konsekuensi dari masing-masing kegagalan yang dianggap perlu pada keluaran elemen diuraikan bersama dengan efek sekunder. Maksud mendefinisikan efek lokal adalah untuk menyediakan dasar untuk penilaian saat mengevaluasi ketentuan alternatif yang ada atau menemukan tindakan perbaikan yang direkomendasikan. Pada keadaan tertentu, tidak boleh ada efek lokal di luar moda kegagalan sendiri.

4.4.3.2 Efek akhir

Saat mengidentifikasi efek akhir, dampak dari satu kegagalan yang dianggap penting pada tingkat sistem tertinggi didefinisikan dan dievaluasi dengan analisis semua tingkat diantaranya. Efek akhir yang diuraikan dapat berupa hasil dari kegagalan ganda. (Misalnya, kegagalan dari satu gawai keselamatan mengakibatkan efek akhir yang katastrofis hanya pada saat gawai keselamatan gagal dan fungsi utama gawai keselamatannya yang didesain

bekerja melampaui batas yang diijinkan) Efek akhir hasil dari kegagalan ganda ditunjukkan pada kertas kerja.

4.5 Metoda deteksi kegagalan

Metoda deteksi moda kegagalan diuraikan. Moda kegagalan selain dari yang sedang dipertimbangkan dan menyebabkan indikasi yang identik dianalisis dan disusun dalam daftar. Kebutuhan untuk deteksi kegagalan yang terpisah pada elemen yang redundan selama operasi sebaiknya dipertimbangkan.

4.6 Pernyataan kualitatif tentang kepentingan kegagalan dan ketentuan alternatif

Arti relatif dari kegagalan sebaiknya dicatat di lembar kerja. Juga dicatat di lembar kerja identifikasi dan evaluasi setiap cirri desain pada tingkat sistem tertentu untuk ketentuan yang lain guna mencegah atau mengurangi efek moda kegagalan. Jadi lembar kerja ini menunjukkan secara jelas perilaku yang sebenarnya dari perlengkapan saat ada malfungsi internal. Ketentuan lain termasuk:

- subsistem redundan yang membolehkan operasi berlanjut jika satu atau lebih elemen gagal;
- sarana operasi alternatif;
- gawai pantau atau alarm;
- setiap saran lain yang membiarkan operasi efektif atau membatasi kerusakan.

Selama tahap desain elemen fungsional (perangkat keras dan perangkat lunak) dari perlengkapan dapat disusun ulang atau dibentuk ulang untuk merubah kemampuannya. Berikutnya, moda kegagalan terkait sebaiknya dikaji ulang sebelum mengulang MKAE.

4.7 Keterangan pada lembar kerja

Jika analisis kekritisitas tidak disetujui untuk dilaksanakan, maka kolom lembar kerja terakhir sebaiknya memberikan keterangan yang terkait untuk mengklarifikasi mengapa tidak disetujuinya untuk dilaksanakan analisis kekritisitas. Rekomendasi untuk perbaikan desain dicatat dan kemudian diperjelas pada kesimpulan. Entri ini dapat termasuk:

- setiap kondisi yang tidak biasa;
- efek kegagalan elemen redundan;
- pengakuan ciri desain kritis yang khusus;
- setiap keterangan untuk memperjelas entri;
- acuan ke entri lain untuk analisis kegagalan yang berurutan.

5 Analisis kekritisitas

Dapat dikehendaki untuk menghitung kekritisitas efek kegagalan dan memperkirakan probabilitas kejadian moda kegagalan terkait. Penghitungan kekritisitas dan probabilitas kegagalan disetujui dilaksanakan sebagai alat bantu untuk pengambilan keputusan pada tindakan perbaikan yang menghasilkan dan skala prioritasnya, dan untuk menetapkan pemisahan yang jelas antara risiko yang dapat diterima dan yang tidak. Masing-masing efek kegagalan yang dipertimbangkan diklasifikasikan menurut kekritisannya terhadap kinerja sistem keseluruhan sesuai persyaratan tujuan, dan keterbatasan sistem. Daftar kegagalan yang kritis harus didefinisikan untuk masing-masing komponen dari perlengkapan. Namun ada beberapa kategori dan klasifikasi yang secara umum dapat diterima yang dapat

diterapkan pada sebagian besar perlengkapan, didasarkan atas konsekuensi tersebut dibawah ini, yang diklasifikasikan secara kualitatif sesuai tingkat konsekuensinya:

- a) kematian atau luka pada personil operasi atau pada masyarakat;
- b) kerusakan pada perlengkapan luar atau perlengkapan itu sendiri;
- c) kehilangan ekonomi karena kekurangan keluaran atau fungsi;
- d) gagal menyelesaikan tugas karena ketidakmampuan perlengkapan untuk melaksanakan fungsi utamanya.

Contoh skala kekritisian yang diperlihatkan pada Lampiran B didasarkan atas luka, kerusakan perlengkapan dan penurunan fungsi.

Pemilihan kategori kekritisian memerlukan keputusan yang hati-hati dan penuh pertimbangan. Secara jelas semua faktor terkait harus dipertimbangkan karena dampaknya pada evaluasi sistem yang berkaitan dengan faktor seperti kinerja , biaya, jadual, keselamatan dan risiko.

5.1 Probabilitas moda kegagalan

Probabilitas kejadian dari moda kegagalan yang diakui dinilai secara kuantitatif dengan menggunakan perkiraan yang diambil secara analitik. Perkiraan probabilitas suatu moda kegagalan khusus dalam lingkungan operasi khusus memerlukan data base keandalan yang penting secara statistik.

Prakiraan dilaksanakan secara paralel dengan MKAE dan dengan menggunakan data langsung dari sumber yang dikutip.

5.2 Evaluasi kekritisian

Evaluasi kekritisian dapat disetujui untuk dilaksanakan dengan menggunakan kotak-kotak kekritisian yang dengan mudah menunjukkan kategori kekritisian sebagai ordinat dan probabilitas atau frekuensi kegagalan sebagai absis. Dalam contoh pada Gambar 1, probabilitas atau frekuensi , diklasifikasikan secara bebas dalam empat kategori: sangat rendah, rendah, medium dan tinggi. Pada beberapa kasus probabilitas atau frekuensi akan diklasifikasikan secara tak linear.

Jika moda kegagalan sudah diklasifikasikan dan ditetapkan probabilitas atau frekuensinya, maka diidentifikasi di kotak yang tepat pada bagan. Makin jauh kotak ini dari titik asal sepanjang diagonal, makin besar kekritisannya dan makin mendesak kebutuhan untuk tindakan perbaikan. Untuk masing-masing analisis kekritisian, julat probabilitas atau frekuensi yang spesifik harus diidentifikasi untuk masing-masing klasifikasi.

6 Laporan analisis

Laporan tentang MKAE (atau MKAEK) dapat dimasukkan dalam suatu studi yang lebih luas atau dapat berdiri sendiri dan harus mencakup kesimpulan dan catatan analisis yang terinci.

Kesimpulan harus mencakup uraian singkat tentang metoda analisis dan tingkat pelaksanaan, asumsi dan aturan pokok. Sebagai tambahan harus termasuk daftar berikut:

- rekomendasi ditujukan kepada pendesain, staf pemeliharaan, perancang dan pengguna;
- kegagalan yang awalnya terjadi sendirian, kemudian menyebabkan efek yang serius;
- perubahan desain yang sudah disatukan sebagai hasil MKAE (atau MKAEK).

Tabel 1 Contoh satu set moda kegagalan umumnya

1	Operasi prematur
2	Kegagalan operasi pada waktu yang ditentukan
3	Kegagalan berhenti operasi pada waktu yang ditentukan
4	Kegagalan selama operasi

Tabel 2 Moda kegagalan generik

1	Kegagalan struktur (pecah)	18	Aktuasi palsu
2	Terikat secara fisik atau macet	19	Gagal berhenti
3	Getaran	20	Gagal memulai
4	Gagal berposisi tetap	21	Gagal menyakelar
5	Gagal membuka	22	Operasi premature
6	Gagal menutup	23	Operasi tertunda
7	Gagal terbuka	24	Masukan salah (kelebihan)
8	Gagal tertutup	25	Masukan salah (kekurangan)
9	Bocor internal	26	Keluaran salah (kelebihan)
10	Bocor eksternal	27	Keluaran salah (kekurangan)
11	Gagal di atas toleransi	28	Kehilangan masukan
12	Gagal dibawah toleransi	29	Kehilangan keluaran
13	Operasi tak sengaja	30	Hubung pendek (listrik)
14	Operasi berselang	31	Terbuka (listrik)
15	Operasi tak beraturan	32	Arus bocor (listrik)
16	Penunjukan yang salah	33	Kondisi kegagalan unik lainnya yang dapat diterapkan pada karakteristik, persyaratan dan keterbatasan operasi sistem
17	Aliran terbatas		

Tingkat kekritisan	IV				
	III				
	II				
	I				
		Sangat rendah	Rendah	Sedang	Tinggi
Probabilitas kegagalan					

Gambar 1 Contoh kotak-kotak kekritisan

Lampiran A
Contoh moda kegagalan, efek dan analisis kekritisan

Tanggal

Kode No..... Nama analis..... Nama enjinir desain.....

Nama Perleng- kapan	Fungsi	Nomor Identi- fikasi	Mode kegagalan	Sebab ke kegagalan	Efek kegagalan		Deteksi kegagalan	Ketentuan aletrnatif	Probabilitas kegagalan	Tingkat Kekritisan	Keterangan
					efek lokal	Efek Akhir					

Lampiran B
Contoh skala kekritisian efek kegagalan

Tingkat Kekritisian	Kondisi kekritisian
IV	Setiap kejadian yang mungkin dapat menyebabkan kehilangan fungsi sistem primer yang mengakibatkan kerusakan berarti pada sistem atau lingkungannya, dan atau menyebabkan hilangnya nyawa atau anggota badan
III	Setiap kejadian yang mungkin dapat menyebabkan kehilangan fungsi sistem primer yang mengakibatkan kerusakan berarti pada sistem tertentu atau lingkungannya dan bahaya terhadap kehidupan dan anggota badan dapat diabaikan
II	Setiap kejadian yang menurunkan fungsi kinerja sistem tanpa kerusakan yang berarti pada sistem atau kehidupan atau anggota badan
I	Setiap kejadian yang dapat menyebabkan penurunan fungsi kinerja sistem yang mengakibatkan kerusakan yang dapat diabaikan pada sistem atau lingkungannya; dan tidak merusak kehidupan atau anggota badan